09-51

CTC
COMMUNICATIONS ENGINEERING & ANALYSIS FOR THE PUBLIC INTEREST

Columbia Telecommunications Corporation • 10613 Concord Street • Kensington, MD 20895
301.933.1488 • fax: 301.933.3340 • www.CTCnet.us

September 30, 2009

Ms. Jennifer Manner
Deputy Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission
Washington, DC 20554

Dear Ms. Manner:

Thank you again for the invitation to participate in the FCC's Public Safety and Homeland Security Workshop on August 25, 2009. It was a privilege to attend and take part.

As requested, I am responding to additional questions you sent on September 11, 2009. I have selected the questions that pertain most closely to my areas of expertise:

- Please explain how "Reverse–911" would be used on an IP based broadband communications network. What bandwidth concerns would there be? What enhanced opportunities are there for conveying emergency information to non-English speaking populations or persons with disabilities?

An IP network provides opportunities for Reverse 911, as well as a broader range of technologies that serve the same purpose as Reverse 911. As with 911, IP telephone users would need to actively register their numbers and addresses with the emergency authorities to receive Reverse 911 calls. The registration process would allow telephone users to indicate whether they have disabilities and what language they need for the calls. The registration process would also provide an opportunity for the recipient to register mobile phone numbers and e-mail accounts for mobile calls, SMS (text) messaging, and subscription-based e-mail, which are already used by many local governments. E-mail and text messaging use less bandwidth, can be communicated to large populations more quickly, and are more likely to be successfully transmitted in an emergency when communications systems are heavily saturated. Also, e-mail and text messaging can be easily translated into multiple languages, provide rich information, and potentially also provide links to more detailed information or media.

Reverse 911 has significant limitations, however. Even if landline directories were accurate and up to date, fewer people have landlines today, and even fewer will pick up their phone for an unknown number. Some mobile telephone operators have delayed or blocked emergency text messages sent by local governments, mistaking them for spam. It is critical that any Reverse 911 or other emergency notification system be tested regularly, and that the operators work with government entities to address technical problems.

- Currently, it seems more profitable for industry to respond to emergencies as they arise than to proactively put emergency infrastructure in place. What are some ways the government can incentivize industry to enhance public safety communications infrastructure?

It will not always be profitable to have infrastructure that is prepared for emergencies. The cost of infrastructure rises with the level of robustness and redundancy built in. The most critical infrastructure should have some type of baseline physical path redundancy, backup power, and physical security—these would be the key public safety locations and wireless/cellular infrastructure. Path redundancy can be accomplished with two fiber paths or with a second wireline or wireless path, as long as there is sufficient capacity available over both routes. Battery backup can be obtained through batteries and generators. There can be some reliance on generators moved into position in an emergency, as long as there are enough generators and a credible way for them to be moved to the site during the emergency. Current FCC rules require eight hours of backup power at wireless base station sites and 24 at central offices[1]—but this is not sufficient for hurricanes, severe ice storms, and other events that can interrupt power for over a week and block roads.

One approach might be to make existing rules more stringent. Another might be to work with standards organizations and industry to develop an independent infrastructure robustness certification that network operators could receive and advertise, based on the actual demonstrated robustness of their network—certification could entitle the operators to tax advantages, reimbursement of some costs, and preference in obtaining government services contracts.

The worst events, such as Hurricane Katrina, will eliminate most terrestrial communications and will require the use of satellites and the capability to place emergency backbone communications into place after the event, potentially using point-to-point wireless and portable wireless base stations. Post-event infrastructure and procedures should also be required and included in evaluating network robustness.

- In regards to discussion on potential conflicts between network neutrality and emergency communications capabilities, if commercial services are to be used for public safety purposes should net neutrality principles apply only to the public internet? How could network neutrality principles allow for managed services for first responders and homeland security users, and would risk based assessment determine service priority?

Using the definition of network neutrality in the "Four Freedoms"[2] as well as the additional two freedoms (nondiscrimination and transparency) proposed by Chairman Genachowski on September 21, 2009,[3] the principle of network neutrality has no bearing on whether first

[1] Code of Federal Regulations, Title 47, Chapter I, Part 12, Section 12.2.

[2] FCC 05-151, Policy Statement, Adopted August 5, 2005.

[3] "FCC CHAIRMAN JULIUS GENACHOWSKI OUTLINES ACTIONS TO PRESERVE THE FREE AND OPEN INTERNET," September 22, 2009, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-293567A1.pdf

responders and homeland security users can obtain service priority. If commercial services are used for public safety and homeland security purposes, the public safety user entities are customers of the network. Public safety and homeland security entities essentially would have a spectrum block or a guaranteed amount of capacity, potentially with the capability to increase that capacity in an emergency.

Regarding the right to "access the lawful Internet content of their choice . . . to run applications and use services of their choice, subject to the needs of law enforcement . . . to connect their choice of legal devices that do not harm the network . . . to [have] competition among network providers, applicant and service providers, and content providers[4] . . . to discriminate against particular Internet content or applications," or to inform subscribers about their network management practices,[5] assigning priority to first responders does not impose, any more than adding any other traffic or customers the network. The speed of the network might be slower for the public than it would otherwise be, in the absence of the first responder use, but there would be a limit on the available capacity in any case, and the added slowness would be non-discriminatory and even. As long as government and network operators had transparent agreements regarding the public safety and homeland security usage, assigning priority to those users should not conflict with the principles of network neutrality.

- What privacy concerns exist for public safety's use of Broadband data when sharing the network with commercial networks? If public safety shared the network with commercial entities beyond normal security measures, what technologies exist that could be put in place to increase security for broadband for emergency responders? How much overhead would data encryption add to speed of transmission?

In most cases, the most sensitive public safety communications will need to be encrypted, even over private networks. The most significant performance impact of encryption on information over a network is the added latency. This will be seen by the public safety user mostly as reduced quality of live video and voice communications, unless the problem was mitigated by high-speed encoding equipment used at the user locations. The amount of added capacity necessary would not be a major consideration, likely in the range of 10%.

Please do not hesitate to get in touch if you have questions or if I can be of further assistance.

Sincerely yours,

Andrew Afflerbach, Ph.D.
Director of Engineering/CEO

[4] FCC 05-151, Policy Statement, Adopted August 5, 2005.

[5] "FCC CHAIRMAN JULIUS GENACHOWSKI OUTLINES ACTIONS TO PRESERVE THE FREE AND OPEN INTERNET," September 22, 2009, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-293567A1.pdf